ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 12/28/2006
2. CONTRACT NO. (if any): HSHQDC-06-D-00026
3. ORDER NO.: HSBP1007J14516
4. REQUISITION/REFERENCE NO.: 0020024860
5. ISSUING OFFICE (Address correspondence to)
   Department of Homeland Security
   Customs & Border Protection
   1300 Pennsylvania Ave., NW
   NP 1310
   Washington DC 20229

6. SHIP TO:
   a. NAME OF CONSIGNEE: See Attached Delivery Schedule
   b. STREET ADDRESS
   c. CITY
   d. STATE
   e. ZIP CODE
   f. SHIP VIA

7. TO:
   a. NAME OF CONTRACTOR: SCIENCE APPLICATIONS INTL CORP
   b. COMPANY NAME
   c. STREET ADDRESS: 8301 GREENSBORO DR, SUITE 860
   d. CITY: McClean
   e. STATE: VA
   f. ZIP CODE: 22102

8. TYPE OF ORDER
   [ ] a. PURCHASE - Reference Your _____
   Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
   [X] b. DELIVERY - Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
   See attached accounting data
   CONTRACTOR TIN: b(4)

10. REQUISITIONING OFFICE
    b(6)

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
    [ ] a. SMALL
    [X] b. OTHER THAN SMALL
    [ ] c. DISADVANTAGED
    [ ] d. WOMEN-OWNED
    [ ] e. HUBZone
    [ ] f. EMERGING SMALL BUSINESS
    [ ] g. SERVICE-DISABLED VETERAN-OWNED

12. F.O.B. POINT: Destination

13. PLACE OF
    a. INSPECTION
    b. ACCEPTANCE

14. GOVERNMENT B/L NO.

15. DELIVER TO F.O.B POINT ON OR BEFORE (Date): 12/31/2007

16. DISCOUNT TERMS: NET 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QTY Accpt (g)
00010	ESS Contract Support for STP (Direct)	1.00	AU	b(4)	b(4)	
00020	ESS Contract Support for STP (COPS)	1.00	AU			

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.

21. MAIL INVOICE TO:
    a. NAME: DHS - Customs & Border Protection National Finance Center
    b. STREET ADDRESS (or P.O. Box): P.O. Box 68908
    c. CITY: Indianapolis
    d. STATE: IN
    e. ZIP CODE: 46268

17(h) TOT. (Cont. pages): $0.00

17(i) GRAND TOTAL: $7,386,547.00

22. UNITED STATES OF AMERICA
    BY (Signature) b(6)
    AUTHORIZED

23. NAME (Typed): Linda Krough
    TITLE: CONTRACTING/ORDERING OFFICER

Previous edition not usable

OPTIONAL FORM 347 (REV. 3/2005)
Prescribed by GSA/FAR 48 CFR 53.213 (e)

Federal Tax Exempt ID: 72-0408780

NOTES:

This labor hour type task order (HSBP1007J14516) is issued against the Department of Homeland Security's (DHS) Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) contract, contract number HSHQDC-06-D-00026. All terms and conditions of both the Customs and Border Protection (CBP) task order and the DHS EAGLE contract are in effect.

This task order is issued for Enterprise Security Services for the Office of Information and Technology, in accordance with the attached Statement of Work (SOW) and SAIC's Price Proposal dated 11/14/2006.

The SOW and Price Proposal are hereby incorporated into this task order.

The Base Period of Performance for this task order is 01/01/2007 - 12/31/2007.

The Ceiling Price for the Base Period is $7,386,547.00.

All labor rates are fixed unit prices.

Option Period I Period of Performance:
01/01/2008 - 12/31/2008
Estimate: $ 7,605,274.00

Option Period II Period of Performance:
01/01/2009 - 12/31/2009
Estimate: $ 7,837,075.00

Option Period III Period of Performance:
01/01/2010 - 12/31/2010
Estimate: $ 8,072,525.00

Option Period IV Period of Performance:
01/01/2011 - 12/31/2011
Estimate: $ 8,279,597.00

The total ceiling amount of this task order is $39,181,018.00 (Base Period plus 4 Option Periods).

b(6) [redacted] is the designated Contracting Officer's Technical Representative (COTR) for this Task Order.

Please submit all invoices to each of the following:

U.S. Customs and Border Protection
Attention: b(6) [redacted]
7681 Boston Blvd

DATE OF ORDER	CONTRACT NO. (if any)	ORDER NO.	PAGE OF PAGES
12/28/2006	HSHQDC-06-D-00026	HSBP1007J14516	3 3

NOTES:

NDC4 Room 109
Springfield, VA 22153

DHS- Customs and Border Protection
National Finance Center
(Address in Section 17 of this task order).

ITEMS AND PRICES, DELIVERY SCHEDULE AND ACCOUNTING DATA
FOR
DELIVERY ORDER: HSBP1007J14516

SCHEDULE OF SUPPLIES/SERVICES

Item Number: 00010 **Line Item (Priced/Information/Option):** P
Supplies/Services: ESS Contract Support for STP (Direct)

Qty	Unit	Unit Price	Ext. Price
1	AU	b(4) [redacted]	b(4) [redacted]

Item Number: 00020 **Line Item (Priced/Information/Option):** P
Supplies/Services: ESS Contract Support for STP (COPS)

Qty	Unit	Unit Price	Ext. Price
1	AU	b(4) [redacted]	b(4) [redacted]

Total Funded Contract Value: $7,386,547.00

ACCOUNTING AND APPROPRIATION INFORMATION

Item: 00010 6100.2525USCSGLCS0923030300Z00007400HQ01 IR2302525 **Amount** b(4) [redacted]

Item: 00020 6100.2525USCSGLCS0923030300Z00007164HQ01 IR2012525 **Amount** b(4) [redacted]

DELIVERY SCHEDULE

==========

Deliver To: Customs and Border Protection

7681 Boston Blvd
VA95 Bus Pk
Springfield VA 22153

Instructions:

Item	Quantity	Delivery Date	Recipient	Unloading PT.
00010	1	01/01/2007		
00020	1	01/01/2007		

Statement of Work
Enterprise Security Service (ESS) Support
for
Bureau of Customs and Border Protection (CBP)
Office of Information and Technology (OIT)
Program Integration Division (PID), Security and Technology Policy Branch (STP)

1.0 Background

The Bureau of Customs and Border Protection (CBP), Office of Information and Technology (OIT), Program Integration Division (PID), Security and Technology Policy Branch (STP), is responsible for providing enterprise security service (ESS) support to CBP and the Department of Homeland Security (DHS).
This support includes, but is not limited to, the following:

- Certification and Accreditation (C&A) support for systems and applications.
- Risk assessments of CBP and select Department of Homeland Security (DHS) sites, as needed.
- Promoting DHS Sensitive System Policy Directives 4300B.
- Identifying and analyzing security risks and mitigation solutions.
- Governing and enforcing security policies.
- Communication Security (COMSEC).
- Developing CBP information system security policies, standards and procedures for both CLASSIFIED and Sensitive but Unclassified (SBU) systems.
- Liaison activities within CBP, the Department of Homeland Security, other government agencies including law enforcement agencies, the international trade community and private firms as they relate to security compliance issues, security programs, policies, issues and products.
- Security architecture development and oversight.
- Training support to the Office of Training and Development (OTD) as Subject Matter Experts.

DHS Chief Information Officer (CIO) has mandated 100 percent certification and accreditation of all DHS Major Applications (MA) and General Support Systems (GSS). The DHS Chief Information Security Officer (CISO) tracks each DHS component's C&A progress. In order to standardize the C&A effort throughout DHS, DHS has mandated the use of two software products: Risk Management System (RMS) and Trusted Agent FISMA (TAF). Only artifacts created using DHS mandated software shall be accepted for credit. STP works on a program-by-program basis, to assure all the systems security documentation and information is complete and ready for the CBP C&A process.

2.0 Scope of Work

The scope of this Statement of Work (SOW) encompasses contractor development of a program to provide enterprise-wide systems security support to STP, including, but not limited to; C&A, risk assessments and mitigation strategies, CLASSIFIED Systems, COMSEC, security policy and procedures, security architecture and Security Test and Evaluation.

The contractor shall be accountable for maintaining and reporting accurate and current technical, administrative and financial status of the IT security program, and other related activities. The contractor shall submit this information in periodic status reports described elsewhere in this document.

The contractor shall provide technical and administrative support personnel who are well qualified and are willing to become familiar with the policy and regulations of CBP.

2.1 Personnel Security

All personnel employed by the contractor or responsible to the contractor for the performance of work hereunder shall either currently possess or be able to favorably pass a full-field background investigation (BI) based on information from the prior seven years of employment. Personnel supporting CLASSIFIED and COMSEC tasks shall also possess or shall be able to obtain a Top Secret clearance with Sensitive Compartmented Information (SCI).

The contractor shall submit within ten (10) working days after award a list containing the full name, social security number, and date of birth of those people who shall require background investigation by CBP, and submit such information and documentation as may be required by the Government to have a BI performed. The information provided must be correct and reviewed by the contractor for completeness. Failure of any contractor personnel to pass a BI shall be cause for the candidate's dismissal from the project and replacement by a similar and equally qualified candidate as determined and approved by the COTR. This policy also applies to any personnel hired as replacements during the term of the contract.

In addition to a personnel full-field BI, the contractor shall submit a DD 254 for those employees that require additional background information needed to authorize access to National Security Information. New hires or substitutions of personnel are subject to the CBP BI clearance requirements.

All BI forms must be delivered to the CBP, Office of Information & Technology (OIT), Personnel Security Branch, Workforce Management Group (WMG) before the employee can work on this contract. After WMG reviews and accepts the BI package, they forward it to Internal Affairs (IA) for determination of suitability. Until IA initiates a full-field BI and the contractor employee passes the TECS/NCIC/Credit Check, he/she

will not be issued a badge, must be escorted at all times while on CBP premises, and will not have access to any CBP systems or sensitive information. If the contractor employee passes the initial TECS/NCIC/Credit checks, he/she is granted a "LIMITED" BI, which enables the employee to have a badge and restricted access to sensitive information. With the "LIMITED" he/she no longer requires an escort.

If the contractor employee fails the TECS/NCIC/Credit checks, his/her BI is put into a "DELAY" status and he/she will not be granted any additional access until the full-field BI is completed. If the contractor employee is put into this "DELAY" status, he/she will not be allowed to work on or bill to this contract until the full-field BI has been successfully adjudicated.

WMG estimates that the TECS/NCIC/Credit check procedures may take one (1) month or longer from the time the packet is received. Completion of the full-field BI may take at least another 90 days.

The contractor shall notify the COTR and Contracting Officer via phone, FAX, or electronic transmission, no later than one workday after any personnel changes occur. Written confirmation or phone notification is required. This includes, but is not limited to, resignations, terminations, and reassignments including those to another contract.

The contractor shall notify the CBP OIT WMG of any change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, and terminations. The contractor shall provide the following information to OIT WMG at Tel. (703) 921-6237 and FAX (703) 921-6780:

Full Name
Social Security Number
Effective Date
Reason for Change

3.0 Tasks

3.1 Task Area 1. Certification and Accreditation

The contractor shall provide technical security expertise in planning, preparing and executing certification and accreditation support for Customs & Border Protection. In support of this task, the contractor shall ensure that CBP information systems and technology are secure and meet all applicable security requirements. In attaining this goal, the contractor shall support the Security & Technology Branch with the review and support of certification and accreditation documentation, participation in technical meetings, on-site observations, efficient use of automated accreditation tools and preparation of technical papers.

Each member of the C&A team shall serve as the Certification Agent (CA) and/or the Information Systems Security Officer (ISSO) for several systems, which include CLASSIFIED and SBU major applications and general support systems. However, the team member shall not serve as both the CA and the ISSO for the same Information system. Furthermore, in order to eliminate any conflict of interest, Government Leads shall serve as the Certifying Agents for any systems for which an STP contractor serves as the ISSO. All artifacts in support of the C&A must meet Federal, DHS and CBP requirements.

3.1.1 Certification Agent (CA) Support for Certification and Accreditation (C&A)

The contractor shall provide personnel to perform CA duties in support of the C&A process at CBP. The CA assigned to an Information Technology (IT) system shall serve as the subject matter expert for security. The CA shall be a point of contact in STP to provide security solutions and interpretations of security policies as they relate to specific architectures and projects. The CA shall establish rapport and develop a relationship with the project development team(s). A CA shall typically serve in that role for more than one system. The CA shall perform duties including but not limited to:

- Supporting audits.
- Monitoring timeliness of accomplishment of required actions and documents pertaining to the C&A of the system throughout its lifecycle.
- Ensuring that an Information Systems (IS) security analysis is conducted to determine appropriate security requirements during the design stage of an application.
- Ensuring that the IS design meets a specified set of security requirements.
- Assisting developers in ensuring IS security requirements for all applications comply with all laws and regulations and are appropriate and sufficient.
- Creating the Security Assessment Reports for the C&A process.
- Ensuring IS security plans and other C&A documents are developed for all applications following DHS and CBP mandated procedures and tasks, such as using RMS.
- Providing written justification, when appropriate, to the Chief, STP Branch for approval by the Assistant Commissioner, Office of Information and Technology (OIT) to obtain a written waiver of policy for mandated security features.
- Coordinating with the assigned Information Systems Security Officer (ISSO) on deployment of new systems and modifications of legacy systems.

- Ensuring that the system/application meets the minimum DHS/CBP certification & accreditation standards before a recommendation is made to the CBP ISSM. Once certification recommendation is accepted by CBP ISSM, the contractor shall upload all relevant C&A artifacts onto the DHS-approved repositories (e.g., Trusted Agent FISMA (TAF)).

- Possessing an understanding of how to determine when security discrepancies exist through knowledge of Federal/DHS laws and security policies, as well as current technologies and architectures. These include understanding the comprehension of CBP's mission, tasks and deliverables for process improvement, and overall risk management.

- Identifying improvement for the accreditation process where practical to lessen: processing time; the amount of paperwork; and resources required, to include benchmarking and other process improvement activities.

3.1.2 Information Systems Security Officer (ISSO)

The contractor shall provide personnel to perform ISSO duties in support of the C&A process at CBP. The ISSO shall be a point of contact in STP to provide security solutions and interpretations of security policies as they relate to specific architectures and information systems (IS's). The ISSO shall establish rapport and develop a relationship with the system development team(s) to become a recognized and integral member of the team. An ISSO shall typically serve in that role for more than one project. The ISSO shall perform duties including but not limited to:

- Participate in appropriate actions to certify and accredit each IS.
- Notify the ISSM when an assigned system requires accreditation or reaccreditation.
- Assist in the certification and accreditation of each system.
- Provide policy and technical advice to systems designers, implementers and operators.
- Conduct risk assessments and prepare an appropriate summary of findings for inclusion within the accreditation documentation.
- Conduct self-assessments of the CBP major applications and general support systems, which shall include vulnerabilities identified at contractor/consultant facilities.
- Recommend corrective actions for deficiencies found during system self-assessments (NIST 800-26) reviews and or during any review or monitoring period for the system/application.
- Ensure timely Plan of Actions & Milestones (POA&Ms) are updated and uploaded in the Trusted Agent FISMA tool. (i.e., by March 10, June 10, September 15, and December 10 annually).

- Draft, review and endorse all information systems security plans and other C&A artifacts, not including the Security Assessment Report (SAR). These artifacts include but are not limited to the following:
    - Privacy Threshold Determination
    - Privacy Impact Assessment (PIA)
    - E-Authentication Determination
    - Controls Testing (Security Test and Evaluation (ST&E)) Plan
    - ST&E Plan Test Results
    - System Security Authorization Agreement (SSAA) (for CLASSIFIED systems)
    - Authorization to Operate (ATO) Authorization Letter
    - Self Assessment (National Institute of Standards and Technology Special Publication (NIST SP 800-26) *NIST DRAFT Special Publication 800-26, Revision 1: Guide for Information Security Program Assessments and System Reporting Form*
    - *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) Assessment
    - Risk Assessment
    - System Security Plan
    - Contingency Plan
    - Contingency Plan Test Results
    - Security Test & Evaluation
    - Security Assessment Report
    - Plans of Actions & Milestones (POA&Ms)
    - Authority to Operate Letter

- At the request of CSIRC, assist in the investigation of security violations and incidents.
- Be knowledgeable on current Federal, National, DHS and CBP standards, policies, requirements and procedures.
- Complete/update a NIST SP 800-26 or NIST SP 800 –53 review for each major application or general support system on a yearly basis. Review and update System Security Plan annually and when significant security changes occur

3.2 Task Area 2 - Communications Security (COMSEC)

COMSEC is the system of security measures used to protect classified information or material utilizing cryptographic keying material and equipment. COMSEC measures are taken to deny unauthorized personnel information derived from telecommunications of the U.S. Government concerning national security and to ensure the authenticity of such telecommunications. COMSEC includes cryptography, transmissions security and physical security of communications security material and information.

Currently CBP utilizes the services DHS COMSEC Office of Record (COR). In the future CBP may opt to recreate its own centralized COMSEC COR.

3.2.1 COMSEC Custodian

The contractor shall serve as COMSEC Custodians for accounts specified by the Chief, STP Branch. The contractor shall perform COMSEC Custodian duties including but not limited to:

- Receipt, custody, issuance, safeguarding, accounting for and when necessary, destruction of COMSEC material for offices and/or operating units under their areas of responsibility.
- Maintaining up-to-date records of COMSEC inventory and submitting required accounting reports.
- Administering initial briefing and debriefing to individual users.
- Maintain copies of all briefings and debriefings.
- Undergo required COMSEC training within six months of appointment and update training yearly.
- Programming and local distribution of COMSEC devices such as the Secure Telephone Equipment (STE) and QSEC 2700, a secure cell phone.
- Receipt, loading and management of COMSEC keying material using devices such as the Electronic Key Management System (EKMS), Data Transfer Device (DTD), Simple Key Loader (SKL) and Secure DTD-2000 System (SDS).

3.2.2 COMSEC COR Duties

The contractor shall provide COMSEC COR services related to the distribution, governance and maintenance of keying material, secure phones and other COMSEC equipment. The contractor shall perform duties including but not limited to:

- Manage and perform centralized COMSEC accounting functions for CBP.
- Provide keying material for CBP with the use of EKMS.
- Perform NSA required audits of each COMSEC account in CBP every 18 months to ensure compliance with NSA and DHS policies.
- Provide COMSEC Custodian and COMSEC equipment training.
- Provide a Help Desk for technical and administrative questions.
- Evaluate new COMSEC equipment and fax machines for use by CBP.
- Represent CBP on Intelligence Community and National Security Agency Policy Working Groups and Committees.
- Provide Controlling Authority function for all CBP COMSEC keying material.
- Appoint new COMSEC Custodians.
- Set up new COMSEC accounts.
- Support COMSEC users on the set up of new secure communications circuits to meet mission needs.
- Provide assistance visits to CBP COMSEC accounts.
- Manage centralized maintenance contracts for COMSEC equipment.

- Maintain a pool of COMSEC equipment, to provide immediate replacement of operational equipment for use in establishing emergency circuits and to replace equipment in need of repair.
- Maintain visibility of all COMSEC assets in CBP to allow cross leveling of equipment or to direct a transfer of excess equipment to meet operational requirements.
- Coordinate and manage centralized Memorandum of Agreement (MOA) and funding for Defense Courier Services (DCS) support.
- Provide technical support to CBP to facilitate interoperability of purchases of COMSEC equipment.
- Provide a central Point of Contact (POC) for secure phone service with vendors such as T-Mobile, Verizon and ATT.
- Provide centralized support service for Satellite phone equipment and service.
- Advocate CBP issues with NSA and the Intelligence Community, to ensure the CBP perspective is heard in operational and policy forums.
- Complete documents and updates to databases as required by DHS 4300B, National Security Systems Handbook. The documentation includes but is not limited to: COMSEC account information, COMSEC Custodian training documentation, COMSEC Facilities documentation, COMSEC Material Accounting, and, COMSEC Incident Reports.

3.3 Task Area 3 - System Architecture

3.3.1 ESS System Architecture

STP has an Enterprise Systems Security Catalog (ESSC) application. The contractor shall assist CBP Security and Technology Policy Branch (STP) in the maintenance of the Enterprise Security System (ESS) Architecture through updates to the ESSC, which include but are not limited to design improvements and updates to the contents of the catalog. The contractor shall identify requirements, establish an Enterprise Information System Architecture (EISA) compliant security architecture template and develop a compliant integrated security architecture and technical reference model (TRM).

The integrated security architecture (voice, video and data) shall be developed based on a top-down approach which defines the necessary services to ensure the confidentiality, integrity, availability, access control, accountability and non-repudiation of CBP systems, networks, applications and infrastructure. The architecture shall consist of three main components: functional architecture (security operations concept), security services architecture and a technical reference model. The architecture shall be based on policy, risk and best-practice-driven requirements. The contractor shall ensure that compliance with DHS and other government agencies (OGA) directives is maintained while ensuring the overall interoperability of the all the components of the Enterprise Security System.

Subcomponents of the architecture may include key management, public key infrastructure, intrusion detection and security management infrastructure that shall ensure the effective management of the security components and provide visibility into the infrastructure of the CBP security posture at any given instance.

The technical reference model (TRM) developed as part of the architectural effort shall form the basis for selection of interoperable products, algorithms, services and security applications programming interfaces.

3.3.2 ESS System Design Support

The contractor shall provide support to assess current and emerging technologies for applicability to and compatibility with the EISA and ESS architecture and design. This includes but is not limited to security reviews in support of the Enterprise Architecture Technical Insertion (TI) process.

3.4 Task Area 4 - Technology Policy Administration (includes Section 508)

STP reviews and establishes all IT policy for the CBP Office of Information and Technology (OIT). These policies include the management and security protection of both classified and sensitive information systems and data. STP also assists in the proper implementation of Section 508 Law with respect to electronic and information technology.

3.4.1 Technology Policy

The contractor shall perform the following duties to include, but not limited to:

- Draft, review, update and coordinate CBP reviews and approval of OIT policies to include the CBP Information Security Policies and Procedures Handbook, User Guide and Rules of Behavior.
- Develop the capability to assess and update existing policies and procedures, to ensure they correctly address any new threats to technology, new vulnerabilities and any changes to business operations. The Policy update process shall include receiving and evaluating policy comments from CBP users and organizations.
- Evaluate the effectiveness and adequacy of existing CBP policy as part of the continued monitoring and assessment of the CBP security posture.
- Develop and prepare a response/recommended CBP position to security policy directives and guidance issued by organizations such as Department of Homeland Security, the Office of Management and Budget (OMB), Public Law and the National Institute of Standards and Technology (NIST).
- Assist in developing process improvement procedures.
- Request, collect and prepare information for the STP Monthly Report.

- Monitor and control database for tracking Interconnection Security Agreements.

3.4.2 Section 508

In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities and to encourage development of technologies that will help achieve these goals. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Section 508 (29 U.S.C. 794d), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.

The contractor shall perform the following duties to include but not limited to:

- Assist the CBP Section 508 Coordinator in proper implementation of Section 508 Law.
- Ensure CBP policies adhere to Section 508 Law.
- Provide expert advice and assistance to CBP Program Offices to ensure major applications and general support systems adhere to Section 508 Law.
- Perform Section 508 Training to CBP employees.

3.5 Task Area 5 - Security Risk Assessment

STP is tasked to conduct Security Risk Assessments (SRAs) of its Local Area Network (LAN) systems throughout the United States and the world, as needed. The number of trips scheduled to perform the SRAs should be considerably less since sites in close proximity are assessed in a single trip. In order to assess the overarching security posture of CBP field sites, a sample of CBP field locations are visited in order to identify the likelihood of threats occurring, the controls in place to prevent or minimize exploitation of the vulnerabilities found, and the severity of the impact on the CBP mission of a threat exploiting identified vulnerabilities. The SRA and Report are based on guidance from NIST SP 800-30, NIST SP 800-26 and NIST SP 800-53. The contractor shall perform risk assessments to support such CBP functional areas that require connection to the CBP network.

The contractor shall review a sampling of the following types of CBP field LAN sites:

- Office of Field Operations (OFO) port offices, cargo inspection areas, field offices, airports, and pre-clearance sites;
- OIT field laboratories;
- OIT LANs in the Washington, DC metropolitan area;
- Office of Air and Marine branch offices;

- Office of Border Patrol branch locations;
- Office of International Affairs Container Security Initiative (CSI) sites; and
- Any other DHS component sites as they migrate to the CBP network.

The contractor shall perform duties including but not limited to:

- Support audits by providing information dealing with LAN risk assessments and related methodology.

- Schedule risk assessments based on importance of the site's mission, type of site (e.g., CSI, Pre-Clearance, Border Patrol branch office, ICE, airport, cargo inspection areas, port offices, laboratories, cargo inspection areas, field offices, Air and Marine branch offices, field offices), geographic area of site location (i.e., sampling of sites from each region and system, and size of site (i.e., number of terminals supported by the LAN at the site).

- Plan and coordinate site visit with the field office (i.e., notify them of the planned visit, collect and review all available information and data available at the site (e.g. LAN Continuity of Operations Plan, Physical Security Assessment Report, Floor Plan, Organization Plan, Mission Statement and artifacts from any prior Security Risk Assessment).

- Coordinate network vulnerability scans with the Computer Security Incident Response Center (CSIRC) and review the scans for high-risk network vulnerabilities.

- Perform a physical inspection of the site and minimally interview the LAN administrator, site management, and system users using documented interview questions.

- For each LAN site SRA characterize the organization and mission, identify supporting assets, identify threats, identify existing security controls and vulnerabilities, and map to controls and vulnerabilities to those recommended by NIST SP 800-53 guidance.

- From the data collected from the pre-assessment phase of the SRA, physical inspections, and interviews; determine likelihood of identified threat occurrences, severity of impact on the CBP mission if a vulnerability is exploited, and associated risk ratings. Develop recommendations regarding mitigation strategies for all identified vulnerabilities.

- Within one month of the SRA at the CBP LAN sites, deliver the Security Risk Assessment Report documenting a description of the mission performed at the locations visited, pertinent physical characteristics of the site and its security posture including supporting assets, threats, vulnerabilities, security controls identified.

- Populate a Plan of Action and Milestones (POA&M) table with the significant vulnerabilities identified by each SRA. Capture this information in the SRA database used to track the progress of the remediation.

- Plan and organize monthly POA&M meetings with the organizations that manage each type of site both from a functional and IT perspective.

- At these POA&M meetings, determine and plan the risk mitigation strategies and/or levels of acceptable risk, establish milestones and estimate the time to mitigation/resolution of vulnerabilities.

- Continually track and update milestones until resolution of the vulnerabilities. Include the information in the SRA database and in TAF, the DHS tool. Update TAF on a monthly basis with any changes in status.

3.6 Task Area 6 - Security Test and Evaluation:

The contractor shall perform Security Testing and Evaluation of a select number of the CBP General Support Systems and applications in support of their Certification and Accreditation and continued improvements to the CBP security posture.

- Personnel must have technical expertise in performing security evaluations of all CBP major applications, Operating Systems and network Internet Operating System (IOS). This includes but is not limited to: Microsoft, Solaris and Linux Operating System, Mainframe (Z/OS), Oracle database, Cisco for wired and wireless Local Area Networks (LANs) and Wide Area Networks (WANS).
- Personnel must perform the testing and document the significant findings in the Security Test and Evaluation report. The documentation must include summary of findings, impact of finding, and recommendations for fixes or other security mitigation strategies.

3.7 Task Area 7 - General Tasks

3.7.1 Capability Maturity Model Integrated (CMMi): The contractor shall work in conjunction with the overall CBP effort to achieve an evaluated, Level 3 integrated CMMi rating, capitalizing on the overall management and direction that shall be provided through the contract support provided for the overall CMM effort. The contractor shall identify those areas of the CMM to be included in the CMM effort and ensure that the appropriate processes and practices are included and addressed. This includes supporting the overall effort by participation in process action teams and working groups and through the development or updates of templates, processes, profiles, procedures, practices or other work products that will support security engineering and execution within CBP.

3.7.2 Compliance Measurement: As documented in the Customs Information Systems Handbook (CIS HB) 1400-05B, CBP Security Policy and Procedures

Handbook, and as part of CMM process improvement, the contractor shall assist in the development of metrics appropriate to measure the compliance and state of the CBP security posture and the effectiveness of the audit, assessment and documentation implementation and compliance.

3.7.3 Communications Plan: The contractor shall develop a plan that includes tailored delivery of the CBP security message while establishing the expectation for compliance and the consequences for noncompliance. The communications plan shall be the vehicle to deliver the security message as it relates to areas such as: policy and procedures, architecture, training and incident identification and reporting. The contractor shall utilize all available means to communicate the necessary information, to include: conferences, conference calls, meetings, committees and incorporation into performance evaluation.

3.7.4 Subject Matter Experts for Training: The contractor shall provide subject matter expertise to the Office of Training and Development (OTD). The training material shall be in support of computer security awareness and security practices for all CBP employees and contract personnel involved with operation of computer systems. This support shall include assistance in the creation, evaluation and review of content for training materials.

4.0 Deliverables

4.1 Reports

Deliverable format shall be based on the type of document and shall conform to CBP directives, where appropriate, and be consistent with other similar efforts. Deliverables shall be accurate in presentation, technical content and adherence to accepted elements of style. In addition, deliverables shall be clear and concise; with engineering terms and project management tools used, where appropriate. All graphics shall be easy to understand, properly labeled with legends and be relevant to the supporting narrative. Deliverables must conform to the On-Site Technical Managers' (OTMs') (i.e., Government Team Leads') specifications. The contractor shall provide the COTR and OTM with a copy of all report deliverables furnished under this task order in soft copy via e-mail.

4.2 Status Reports

4.2.1 Weekly Reports

The written weekly report shall consist of a summary of significant events and actions accomplished for the week. A bi-weekly verbal presentation shall consist of the following: actions accomplished for the previous two-week period; actions planned; and any issues of concern that may require special attention. This verbal report shall be presented to the Chief, STP Branch, COTR, and the OTMs on the second and fourth Thursday or as otherwise scheduled by the COTR.

4.2.2 Monthly Report

The contractor shall submit monthly status reports to the COTR and OTMs on progress made during the respective reporting period in performance of the work requirement. The reports shall address work completed during the current period, planned activities, problems/issues with recommended solutions, anticipated delays, and resources expended. The reports shall be sufficiently detailed to provide an ongoing record of all support efforts.

These reports shall be submitted within 5 calendar days following the end of each work month. (Each work month is defined as 30 consecutive calendar days.)

The monthly report shall be delivered in hard copy to the COTR and OTMs. One electronically provided (i.e., via email) soft copy shall be sent to the COTR. The report shall be in a format to be agreed upon with the COTR.

4.2.3 Cost Reports/Invoices

To ensure the timely processing of the contractor's invoices, the contractor shall provide the COTR with copies of timesheets at the end of each timesheet period for each person with hours expended in support of the contract over the reporting period.

Invoices shall contain the following information:

- Date invoice is issued;
- Contract number;
- Period of performance (start and expiration date);
- Funding Source (e.g., Base, CSI, COBRA, and ACS Life Support), which shall be identified to the contractor upon award of the task order.
- For each funding source and task area listed, the contract labor categories and the names of the persons associated with the labor category;
- Contract labor category rate;
- Straight time labor hours by person (regular/extended time [i.e., no overtime charges may be submitted; just straight time] over the period of performance;
- Cumulative straight time labor hours by person (regular/extended time) for contract period of performance;
- Labor sub-totals for each funding category and task area;
- Travel and per diem charges by person for invoice period (with receipts for expenses incurred) and cumulative over the contract period.
- Other Direct Costs (ODCs) incurred during the period of performance with receipts or explanation of each item if no receipt and cumulative ODCs.

Invoices shall include Grand Totals for all funding sources, labor categories, travel and ODCs for the contract. The next pages of the report shall contain the following fields:

Period of performance expiration date, Hours-the number of hours billed against the contract for that month; Cost – this is the amount billed against the contract for that month; Allocated - this is the award amount of the contract (i.e., this is the amount the Government obligated to the contract); Cumulative - this is the amount billed against the contract since the beginning of the contract; PCT - This the percentage billed to date, remaining – This is the amount remaining on the task assuming that month's invoice is approved to date.
The invoice shall contain the following statement signed and dated by an authorized company representative: "This is to certify that the services set forth herein were performed during the period stated."

4.2.4 Invoice Submission

The vendor shall invoice the Government monthly for services performed under the contract. Invoices shall be for services, travel and ODCs incurred against the contract during the previous month's period of performance. The period of performance shall begin on the first of the month and end on the last day of that month. Invoices shall be received by the tenth day of each month and include billable items for the previous month's period of performance. One (1) copy of the invoice document shall be submitted to the COTR at the following address:

Bureau of Customs and Border Protection
7451 Boston Boulevard, NDC4 Rm. 109
Springfield, Virginia 22153
Attn: b(6) [redacted]

Simultaneously, one copy of the invoice shall be mailed to the Contracting Officer at the following address:

Bureau of Customs and Border Protection
Office of Finance, Procurement
ATTN: b(6) [redacted] Contract Specialist
1300 Pennsylvania Avenue, NW
Washington, DC 20229

4.2.5 Invoice Modification

The contractor shall endeavor to ensure that all employee timesheet submissions and all travel receipts are accurate and valid, and as such, the invoices submitted to the Government should not require future changes. In the event that an error is made, the change shall be recorded and invoiced within ninety (90) days of the last day of the month in which the labor or travel was performed or the ODC was purchased. In addition, any such adjustment shall contain detailed documentation explaining the error and the time period during which it occurred. No changes shall be accepted after ninety (90) days of the end of the period of performance.

At the COTR's discretion, the format of the invoice may be changed. The COTR shall notify the contractor of the change in format at least 60 days prior to requiring its use by the contractor.

4.2.6 ODC Process

The contractor shall acquire the COTR or his/her designee's approval on all ODCs prior to initiating any purchase and/or ODC expense. When submitting ODC requests, the contractor should provide details such as which task area it supports and how it will support the task identified.

4.2.7 Travel

All travel shall be in accordance with the Federal Travel Regulations (for travel in 48 contiguous states), the Joint Travel Regulations, DoD Civilian Personnel, Volume 2, Appendix A (for travel to Alaska, Hawaii, Puerto Rico, and U.S. territories and possessions), and the Standardized Regulations (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" (for travel not covered in the Federal Travel Regulations or Joint Travel Regulations).

Travel expenses shall be separately identified on invoices accompanied by all paid receipts during the time of travel.

4.3 Briefings and Meetings

Each briefing/meeting shall cover the essential elements of the relevant subject matter and shall be prepared and presented in a clear, concise, and orderly manner. Appropriate briefing tools such as Microsoft PowerPoint, overhead slides, plotted charts, etc., shall be used. Hardcopy handouts of all briefing materials shall be made available to all attendees prior to, or at the time of, the briefing.

4.3.1 Meetings

a. Kick-Off Meeting/Draft Project Schedule – A task order kick-off shall be scheduled within 10 days after award. Attendees shall be at a minimum: CBP COTR, On-Site Technical Managers (OTMs), Contracting Officer, Program Manager and contractor. The contractor shall provide a draft schedule of their plan to meet the customer's requirements as identified in this statement of work. This shall be due within 10 workdays after award of the task order. Any changes or adjustments to this schedule shall be coordinated with the appropriate OTM.

b. Periodic Meetings: CBP will coordinate periodic meetings and reviews to ensure all relevant provisions of the task order are being met.

4.4 Performance

The contractor shall follow the performance guidelines listed below.

4.4.1 Place of Performance

Work shall be performed primarily at the CBP National Data Center buildings located in Newington, VA, or other CBP locations in the Washington, D.C. metropolitan area and within a 50-mile radius of the D.C. metro area at the discretion of the COTR.

4.4.2 Hours of Operations

All work shall be performed during a normal 40-hour week -- Monday through Friday, with core hours from 9:00 AM until 3:00 PM. Core hours refer to the hours of the day contractors shall work. The contractors shall work no later than 9:00AM. The contractor can start earlier than 9:00 AM but shall not end their day earlier than 3:00PM. Contractors shall take at least 30 minutes for lunch. For example, a contractor must spend 8 hours and 30 minutes at work to claim an 8-hour day.

The technical staff shall work on-site at the government facility unless approval is obtained from the COTR. The contractor staff shall observe the following government holidays unless the COTR approves otherwise:

- Christmas
- New Year's
- Martin Luther King
- President's Day
- Memorial Day
- Independence Day, July 4th
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Inauguration Day (as appropriate)

The contractor staff shall inform the OTMs of all vacations and other time off. The contractor staff shall provide adequate coverage (as determined by OTMs) on all business days – to include weekdays after holidays.

4.4.3 Period of Performance

Base Period	01/01/07 thru 12/31/07
Option Period #1	01/01/08 thru 12/31/08
Option Period #2	01/01/09 thru 12/31/09
Option Period #3	01/01/10 thru 12/31/10
Option Period #4	01/01/11 thru 12/31/11

4.5 Delivery Schedule

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
1	**Kick-Off Meeting/Draft Project Schedule**	4.2.a	Within 10 days after award	Within 10 days of award	OTMs, COTR and Contractor Project Manager
2	**Security Assessment Reports**	3.1.1	As Required	As Required	COTR, applicable OTM
3	**Privacy Impact Assessment (PIA)**	3.1.2	As Required	As Required	COTR, applicable OTM
4	**E-Authentication**	3.1.2	As Required	As Required	COTR, applicable OTM
5	**Controls Testing (Security Test and Evaluation (ST&E)) Plan and Results**	3.1.2	As Required	As Required	COTR, applicable OTM
6	**System Security Authorization Agreement (SSAA) for CLASSIFIED Systems**	3.1.2	As Required	As Required	COTR, applicable OTM
7	**Authorization to Operate (ATO) Letter**	3.1.2	As Required	As Required	COTR, applicable OTM
8	**Self Assessment (NIST SP 800-26)**	3.1.2	As Required	As Required	COTR, applicable OTM
9	**FIPS-199 Assessment**	3.1.2	As Required	As Required	COTR, applicable OTM
10	**Risk Assessment**	3.1.2	As Required	As Required	COTR, applicable OTM
11	**System Security Plan**	3.1.2	As Required	As Required	COTR, applicable OTM
12	**Contingency Plan**	3.1.2	As Required	As Required	COTR, applicable OTM
13	**Contingency Plan Test Results**	3.1.2	As Required	As Required	COTR, applicable OTM
14	**C&A Artifacts and documentation as specified by DHS and/or CBP requirements**	3.1	As Required	As Required	COTR, applicable OTM

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
15	Updated COMSEC Account Database Reports	3.2.1	As Required	As Required	COTR, applicable OTM
16	COMSEC Training - Soft copy of training materials	3.2.2	As Required	As Required	COTR, applicable OTM
17	Documentation and Reports regarding COMSEC Custodian appointments and COMSEC Accounts	3.2.2	As Required	As Required	COTR, applicable OTM
18	Technical Reference Model (TRM) ESSC Catalog Updates and Design Improvements Documentation and Progress Reports	3.3.1	As Required	As Required	COTR, applicable OTM
19	Policy Guides and Handbooks	3.4.1	As Required	As Required	COTR, applicable OTM
20	Section 508 Training Materials	3.4.2	As Required	As Required	COTR, applicable OTM
21	Risk Assessment Security Questionnaire	3.5	As Required	As Required	COTR, applicable OTM
22	Risk Assessment Visit Plans and Process Documentation	3.5	As Required	As Required	COTR, applicable OTM
23	Risk Assessment Reports	3.5	As Required	As Required	COTR, applicable OTM
24	Plans of Action and Milestones Documents	3.5	As Required	As Required	COTR, applicable OTM
25	Security Test and Evaluation Reports	3.6	As Required	As Required	OTM TPOC
26	Communications Plan	3.7.3	As Required	As Required	COTR, applicable OTM

No	Title/Soft Copy Format	SOW Paragraph	Draft Due	Final Due Date	Recipient(s)
27	**Content for Training/Review of Training Material**	3.7.4	As Required	As Required	OTM TPOC
28	**Weekly Reports**	4.2.1	Weekly	Weekly	COTR, applicable OTM
29	**Monthly Reports**	4.2.2	Monthly	Monthly	COTR, applicable OTM
30	**Cost Reports**	4.2.3	Monthly	Monthly	COTR, applicable OTM

The work products are to be delivered in accordance with the schedule set forth in the table above. All documents must be provided in soft copy format to the recipients listed above. In addition, one hard copy should be provided to the OTM. The contractor shall refer to Section 4 Deliverables for work product

4.6 ACCEPTANCE REQUIREMENTS

The on-site technical manager (OTM) shall review all deliverables for accuracy and completeness. The contractor shall make those corrections required by the OTM. The deliverables require acceptance by the appropriate OTM or the COTR.

4.6.1 General Acceptance Criteria

Specific criteria shall be set forth for each task area, if applicable. Accordingly, general quality measures, as set forth below shall be applied to each work product received from the contractor under this SOW.

Accuracy. Work products shall be accurate in presentation, technical content and adherence to accepted elements of style.

Clarity. Work products shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and be relevant to the supporting narrative.

Conformance to Requirements. All work products shall satisfy the requirements of the work request. The product shall adhere to CBP SDLC-based templates, standards and directives.

File Editing. All text and diagrammatic files shall be editable by the Government.

Format. Work products shall be submitted in media defined in Section 4 Deliverables. The work product format may change from subtask to subtask. Hard copy formats shall follow CBP/DHS Directives and shall be consistent with similar efforts.

Timeliness. Work products shall be submitted on or before the due date specified in the Work Request or submitted in accordance with a later scheduled date determined by the Government.

4.6.2 Points of Contact

Contract deliverables shall be provided to the following specific points of contact:

CBP, COTR
Bureau of Customs and Border Protection
7451 Boston Boulevard, NDC4 Rm. 109
Springfield, Virginia 22153
Attn: b(6) [redacted]

OTM:
On-site Technical Managers STP
b(6) [redacted]

5.0 **Level of Effort (Project Staffing Estimates)**

The following estimates are for planning, proposal pricing and evaluation purposes.

Labor Category	FTE	Estimated Hours by Labor Category
Project Manager	b(4)	1,920.00
Subject Matter Expert		1,920.00
Technical Writer/Editor		3,840.00
Administrative Specialists (Senior)		3,840.00
IT Security Specialist (Senior)		19,200.00
IT Security Specialists		34,560.00
Computer Systems Analyst (Senior)		17,280.00
Total	**43**	**82,560.00**

Cost Summary

Base Year (1/1/07 - 12/31/07)			
Labor Category	Proposed Rate	Total Hours	Total Price
Project Manager	b(4)	1,920	b(4)
Subject Matter Expert		1,920	
Technical Writer/Editor		3,840	
Administrative Specialists (Senior)		3,840	
IT Security Specialist (Senior)		19,200	
IT Security Specialist		34,560	
Computer Systems Analyst (Senior)		17,280	
Total Base Year		**82,560**	**$7,386,547**

Option Year I (1/1/08 - 12/31/08)			
Labor Category	Proposed Rate	Total Hours	Total Price
Project Manager	b(4)	1,920	b(4)
Subject Matter Expert		1,920	
Technical Writer/Editor		3,840	
Administrative Specialists (Senior)		3,840	
IT Security Specialist (Senior)		19,200	
IT Security Specialist		34,560	
Computer Systems Analyst (Senior)		17,280	
Total Option Year I		**82,560**	**$7,605,274**

Option Year II (1/1/09 - 12/31/09)			
Labor Category	Proposed Rate	Total Hours	Total Price
Project Manager	b(4)	1,920	b(4)
Subject Matter Expert		1,920	
Technical Writer/Editor		3,840	
Administrative Specialists (Senior)		3,840	
IT Security Specialist (Senior)		19,200	
IT Security Specialist		34,560	
Computer Systems Analyst (Senior)		17,280	
Total Option Year II		**82,560**	**$7,837,075**

Option Year III (1/1/10 - 12/31/10)			
Labor Category	Proposed Rate	Total Hours	Total Price
Project Manager	b(4)	1,920	b(4)
Subject Matter Expert		1,920	
Technical Writer/Editor		3,840	
Administrative Specialists (Senior)		3,840	
IT Security Specialist (Senior)		19,200	
IT Security Specialist		34,560	
Computer Systems Analyst (Senior)		17,280	
Total Option Year III		**82,560**	**$8,072,525**

Option Year IV (1/1/11 - 12/31/11)			
Labor Category	Proposed Rate	Total Hours	Total Price
Project Manager	b(4)	1,920	b(4)
Subject Matter Expert		1,920	
Technical Writer/Editor		3,840	
Administrative Specialists (Senior)		3,840	
IT Security Specialist (Senior)		19,200	
IT Security Specialist		34,560	
Computer Systems Analyst (Senior)		17,280	
Total Option Year IV		**82,560**	**$8,279,597**

Base plus All Option Years (1/1/07 - 12/31/11)			
Labor Category		Total Hours	Total Price
Project Manager		9,600	b(4)
Subject Matter Expert		9,600	
Technical Writer/Editor		19,200	
Administrative Specialists (Senior)		19,200	
IT Security Specialist (Senior)		96,000	
IT Security Specialist		172,800	
Computer Systems Analyst (Senior)		86,400	
Total Base plus All Option Years		**412,800**	**$39,181,018**